AMENDMENTS TO THE CLAIMS

Please add or amend the claims to read as follows, and cancel without prejudice or disclaimer to resubmission in a divisional or continuation application claims indicated as cancelled:

1. (**Currently Amended**) A method for protecting the transfer of data ~~from or to~~ between a computer and a device, the method comprising the steps of:

   a. receiving a data portion during a data communication session, the data portion being associated with a particular physical communication port of the computer and with the device that is currently communicating via the particular physical communication port;

   b. processing the data portion according to a protocol that is associated with the physical communication port;

   c. determining whether a decision on the data communication session may be reached, if not storing the data portion in a buffer, wherein the buffer is associated with the data communication session and returning to step 'a' ~~to wait~~ and waiting for the next data portion, if yes, proceed to step 'd';

   d. determining whether to allow the data communication session, if yes transferring the one or more data portions with data that are stored in the associated buffer, if any exist, toward or from the physical communication port, if not modifying the data transportation.

2. (Original) The method of claim 1, wherein the step of modifying the data transportation further comprises blocking the transportation.

3. (Original) The method of claim 1, wherein the step of modifying the data transportation further comprises modifying the type of the transportation.

4. (Original) The method of claim 1, wherein the step of modifying the data transportation further comprises modifying the status of a requested file.

5. (Original) The method of claim 1, wherein the step of modifying the data transportation further comprises correcting the data according to the communication protocol.

6. (Original) The method of claim 1, wherein the physical communication port is selected from a group consisting of SCSI bus, Serial, Parallel, FireWire, PCMCIA bus, cellular, fiber channel, Bluetooth, iSCSI, Infiniband, and Infrared.

7. (Original) The method of claim 1, wherein the physical communication port is a USB port.

8. (Original) The method of claim 1, wherein the physical communication port is wireless.

9. (Original) The method of claim 1, wherein the step of processing the data portion further comprising:

(i) determining whether additional processing based on a higher level protocol is required, and if not continuing at step 'c', otherwise continue at step (ii); and

(ii) processing part of the data portion that is relevant to the higher level protocol according to the higher level protocol and returning to step (i).

10. (**Currently Amended**) The method of claim 9, wherein the step of processing part of the data portion further comprises processing relevant to a higher level protocol that is associated with [[a]] the device ~~selected from a group of devices consisting of flash memory, removable hard disk drive, floppy disk, writable CD-ROM, a PDA, a cellular phone, a WiFi dongle and a Bluetooth dongle~~.

11. (**Currently Amended**) The method of claim [[9]] 10, wherein the ~~higher level protocol~~ device is ~~associated with~~ an application selected from a group consisting of synchronization applications for PDA, Java applications for synchronization with cellular phone, backup storage applications, Bluetooth and WiFi protocols.

12. (Original) The method of claim 1, wherein the step of processing the data portion is performed in respect of the data that is stored in the associated buffer.

13. (Original) The method of claim 1, wherein the step of determining whether a decision on the data communication session may be reached, is performed in respect of the data that is stored in the associated buffer.

14. (Original) The method of claim 1, wherein the step of determining whether a decision to allow the data communication session is performed in respect of the data that is stored in the associated buffer.

15. (Original) The method of claim 1, wherein the step of receiving a data portion further comprises receiving a data portion that is selected from a group consisting of packet and SCSI block.

16. (Original) The method of claim 1, wherein the step of receiving the data portion further comprises obtaining the data portion by emulating a class driver.

17. (Original) The method of claim 1, wherein step of receiving the data portion further comprises obtaining the data portion by emulating a filter module.

18. (Original) The method of claim 1, wherein the step of processing the data portion according to a protocol that is associated with the physical communication port further comprises:

i. parsing the data portion;
ii. reassembling the data; and
iii. analyzing the reassembled data.

19. (Original) The method of claim 1, wherein the step of determining whether to allow the communication session further comprises reviewing the security policy.

20. (Original) The method of claim 1, wherein the step of determining whether to allow the communication session further comprises examining the working environment in which the computer is operating and only allowing the communication for certain working environments.

21. (**Currently Amended**) A system for enhancing the security of a private network being accessed by a computer, the system comprising:

a client agent that is communicatively coupled to the private network and is associated with a computer operating on the private network, the client agent having an associated security policy;

a security manager that is communicatively coupled to the private network;

the client agent being operative to:

detect a data transfer passing between a device connected to the computer through ~~at least one~~ a physical communication port of the computer;

analyze the data transfer according to the communication protocol associated with the ~~at least one~~ physical communication port; and

verify the data transfer is allowable based on the analysis of the data and the security policy; and

the security manager being operable to associate a security policy with the client agent.

22. (Original) The system of claim 21, wherein the security manager is operable to verify that the security policy is correct.

23. (Original) The system of claim 21, wherein the security policy includes a plurality of rules that at least define limits on data transfers during a communication session.

24. (Original) The system of claim 21, wherein the security policy includes a plurality of rules that at least define the type of operations that can be performed during a communication session.

25. (**Currently Amended**) The system of claim 21, wherein the security manager is operable to disable any communication ~~between~~ with the computer ~~and the private network~~ unless the client agent associated with the computer is active.

26. (**Currently Amended**) The system of claim 21, wherein the ~~at least one~~ physical communication ports can be selected from a group consisting of SCSI bus, Serial, Parallel, FireWire, PCMCIA bus, cellular, fiber channel, Bluetooth, iSCSI, Infiniband, and Infrared.

27. (**Currently Amended**) The system of claim 21, wherein the ~~at least one~~ physical communication ports is a USB port.

28. (**Currently Amended**) The system of claim 21, wherein the ~~at least one~~ physical communication ports is wireless.

29. (Original) The system of claim 21, wherein the client agent is associated with the security policy by loading the security policy into the client agent.

30. (Original) The system of claim 21, wherein the security manager is operable to verify that the security policy loaded into the client agent has not been modified.

31. (Original) The system of claim 21, wherein the client agent is further operative to transmit a report to the security server, the report identifying events that occurred with the computer in view of the security policy.

32. (Original) The system of claim 21, wherein the client agent is operable to analyze the data based on a higher level protocol that is associated with a device selected from a group consisting of flash memory, removable hard disk drive, floppy disk, writable CD ROM, a PDA, a cellular phone, a WiFi dongle and a Bluetooth dongle.

33. (Original) The system of claim 21, wherein the client agent is operable to analyze the data based on a higher level protocol that is associated with an application selected from a

group consisting of synchronization applications for PDA, Java applications for synchronization with cellular phone, backup storage applications, Bluetooth and WiFi protocols.

34. (Original) A software agent installed in a computer for enhancing the security of the computer, the agent being operative to:

detect a data transfer passing through at least one physical communication port of the computer;

analyze the data transfer according to the communication protocol associated with the at least one physical communication port; and

verify the data transfer is allowable based on the analysis of the data and a security policy.

35. (**New**) The method of claim 10, wherein the device is a device selected from a group of devices consisting of flash memory, removable hard disk drive, floppy disk, writable CD ROM, a PDA, a cellular phone, a WiFi dongle and a Bluetooth dongle.